Extreme Networks Solutions Selling: ExtremeManagement Knowledge Transfer

Abstract: This document has been created for the use of Extreme Networks SEs and Partners. The primary purpose of this document is to serve as textbook style training material used in conjunction with the ExtremeManagement 200 level training course. The content in this particular document focuses on the transfer of technical knowledge necessary to provide Extreme SEs and partners foundational knowledge supporting the technical skillsets required to design an ExtremeManagement system.

Published: February 2018

Extreme Networks, Inc.
145 Rio Robles
San Jose, California 95134
Phone / +1 408.579.2800
Toll-free / +1 888.257.3000
www.extremenetworks.com

Contents

PaloAlto integration

With Extreme Control the customer does have visibility of each end-system attached to the network = Username, IP, location, … The Firewall is very limited getting information about user location, username, end-system device. We can provide mapping of username-IP to the firewall. Firewall can apply different approach to traffic generated by that IP.

Next Generation firewall can get information about username by:

- Reading Active Directory logs = not every device is in AD (not only managers are happy with Mac)
- Getting the Kerberos protocol information (logging to AD) = kerberos authentication does generate ticket to the user. The ticket is valid for specific time period. If the user moves from wired to wireless or form one zone to other and get new IP address the new ticket is not generated => firewall does not get this information
- Getting the information from the end-system = not every end-system can be reconfigured to support it. Sometimes the way is only through web browser, but not every user does use web browser every time…

Next Generation firewall can block the traffic if the traffic is processed by the firewall only. Firewall cannot block horizontal communication = communication within the subnet not passing the firewall.

Why = Use Cases.

Customer can apply different Firewall Rules, AntiVirus settings, URL filtering, AntiSpyware, File Blocking, Data Filtering, … based on user group. = Different firewall rules for sales team comparing to engineering team, different URL filters for different Contractors…

Firewall is informed by XMC if the end-system is disconnected from the network, so firewall can close all opened sessions. Session can’t be hijacked.

If firewall detects the Spyware or Virus or any kind of threat then XMC will be informed and XMC will perform action at the place where the end-system is connected. Example of such action is applying quarantine security policy profile.

Extreme Policy vs. Firewall

Extreme Policy (One Policy) is applied on the PEP (Policy Enforcement Point) = as close to the end system as possible = usually first port / Access Point where the end system is connected.

Firewall rules are applied inline on the firewall. Firewall is usually placed between two security zones.

Firewall can block the traffic much deeper in the network while Policy is much closer to the edge.

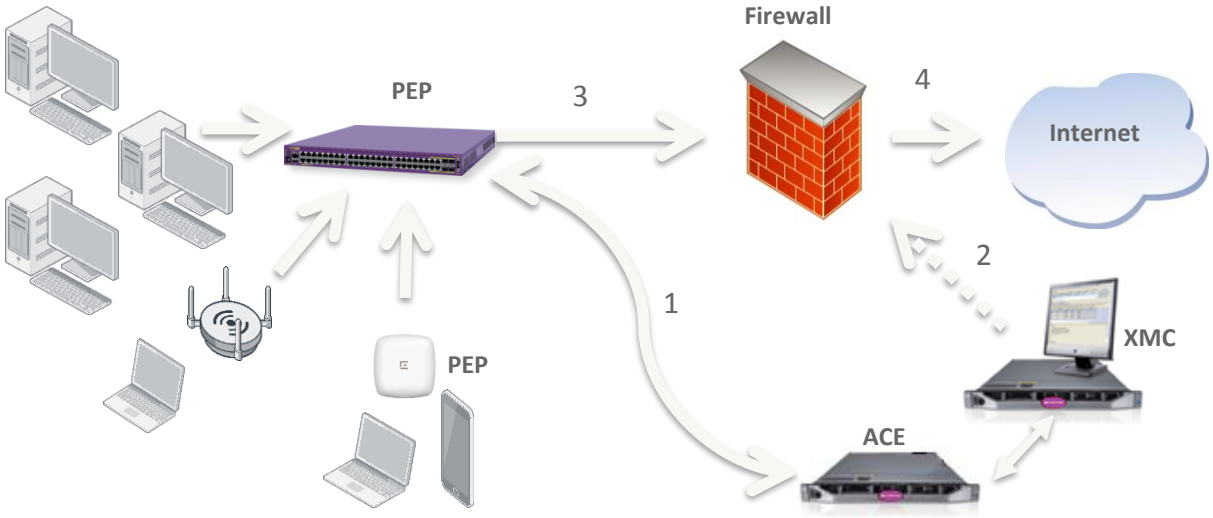
Extreme Policy can apply the QoS, VLAN, Filtering…

Firewall can apply QoS, ACLs, DPI (Deep Packet Inspection) = Antivirus, AntiMallware, Application analytics, firewall rules are statefull.

Policy is applied in ASIC hardware = performance of Tbps for acceptable price, with many ports.

Firewall is software (some do have hardware acceleration) = performance of Gbps, lower number of ports, higher price.

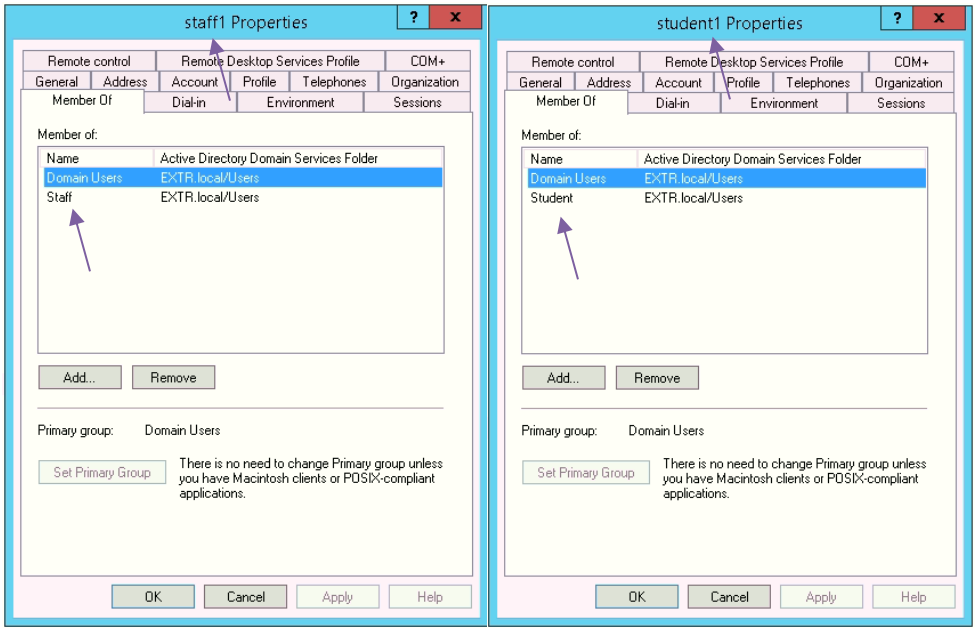
How it works – XMC -> PaloAlto



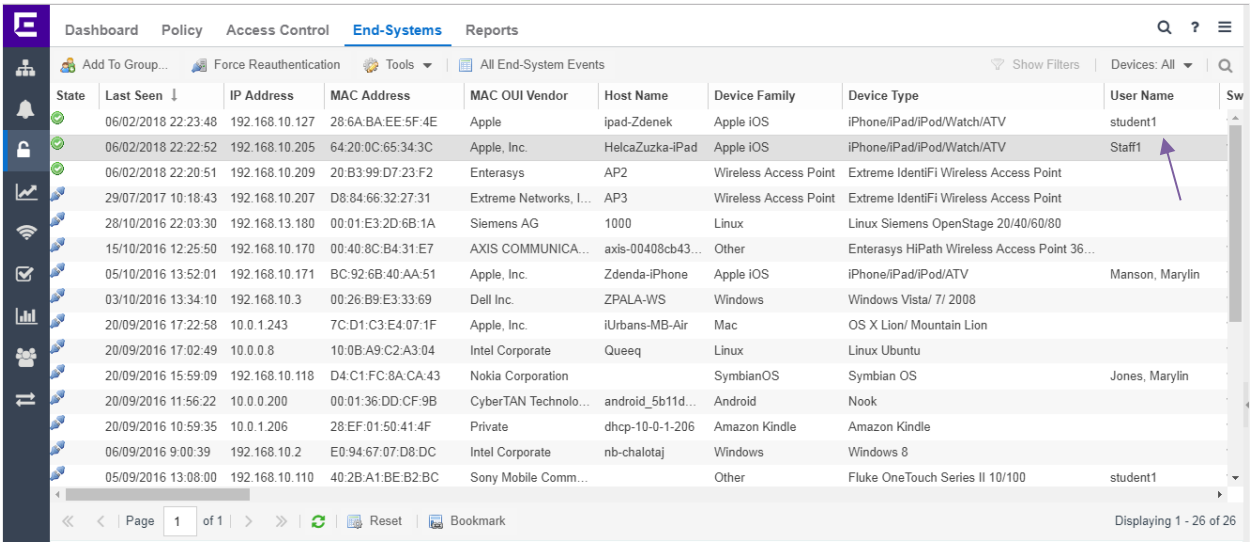
0. End-system connects to the access switch / access point.
1. The radius communication reaches the Access Control Engine. ACE does process configuration rules and based on conditions the Access Control Profile is chosen. Access Control Profile does assign Security Policy Profile. The Radius Access Accept is sent to the access switch / access point. There can be Security Policy Profile in the Radius Access Accept.
2. When the address resolution is finished (the XMC knows the IP address of the end-system) the user-id mapping is sent to the firewall through the API.
3. Firewall does apply its configuration on the traffic from the end-system. Based on the information from the XMC the firewall knows the username for the source IP.
4. Traffic is inspected by the firewall with rules reflecting the Username.

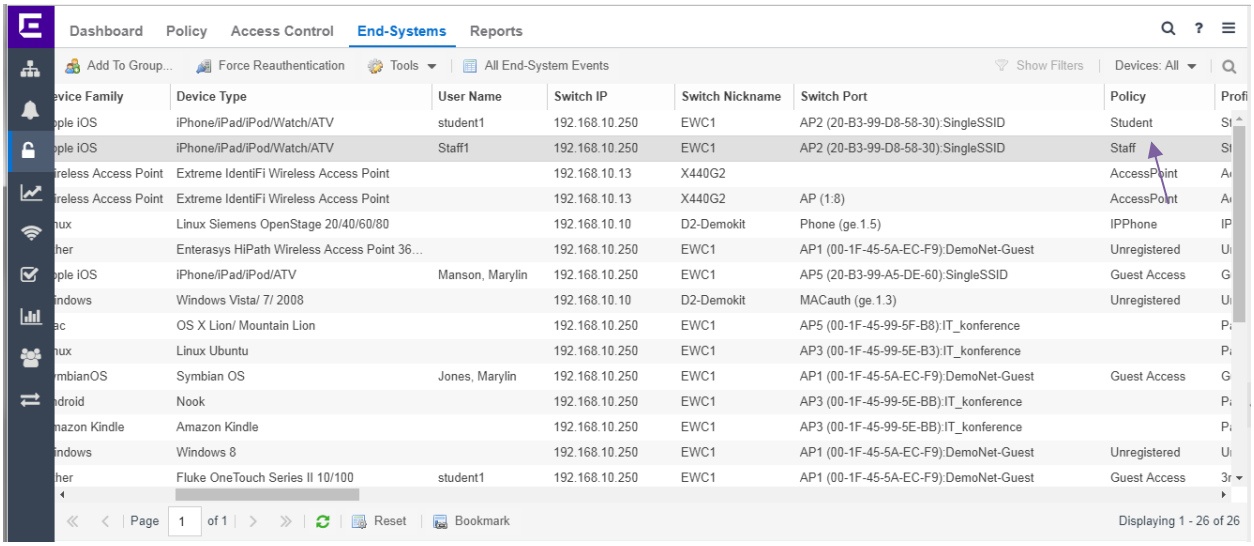
LDAP - > Extreme Control -> Policy -> XMC -> PaloAlto

User “staff1” is part of the “Staff” group in the AD, “student1” is part of “Student” group:

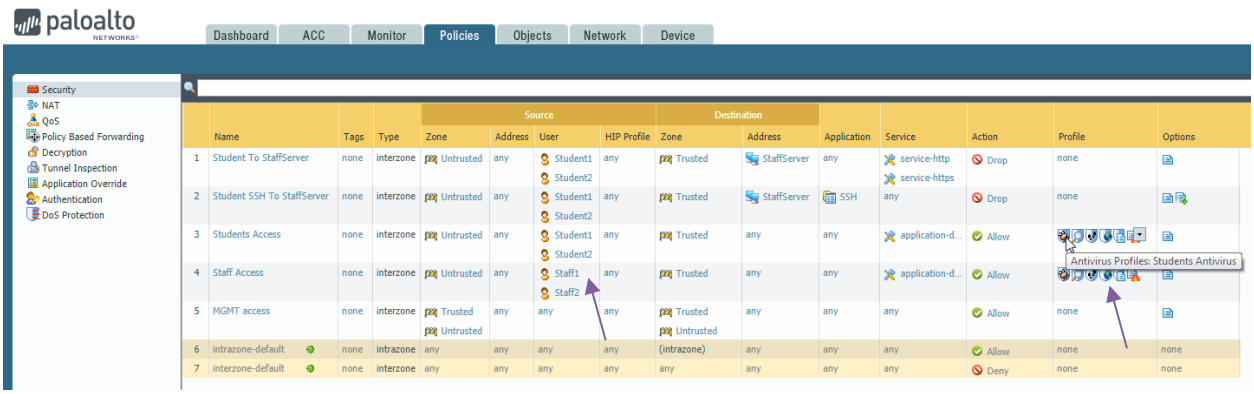


Users are authenticated, IP addresses are resolved, Policy is applied on PEP, security policy profile is assigned:

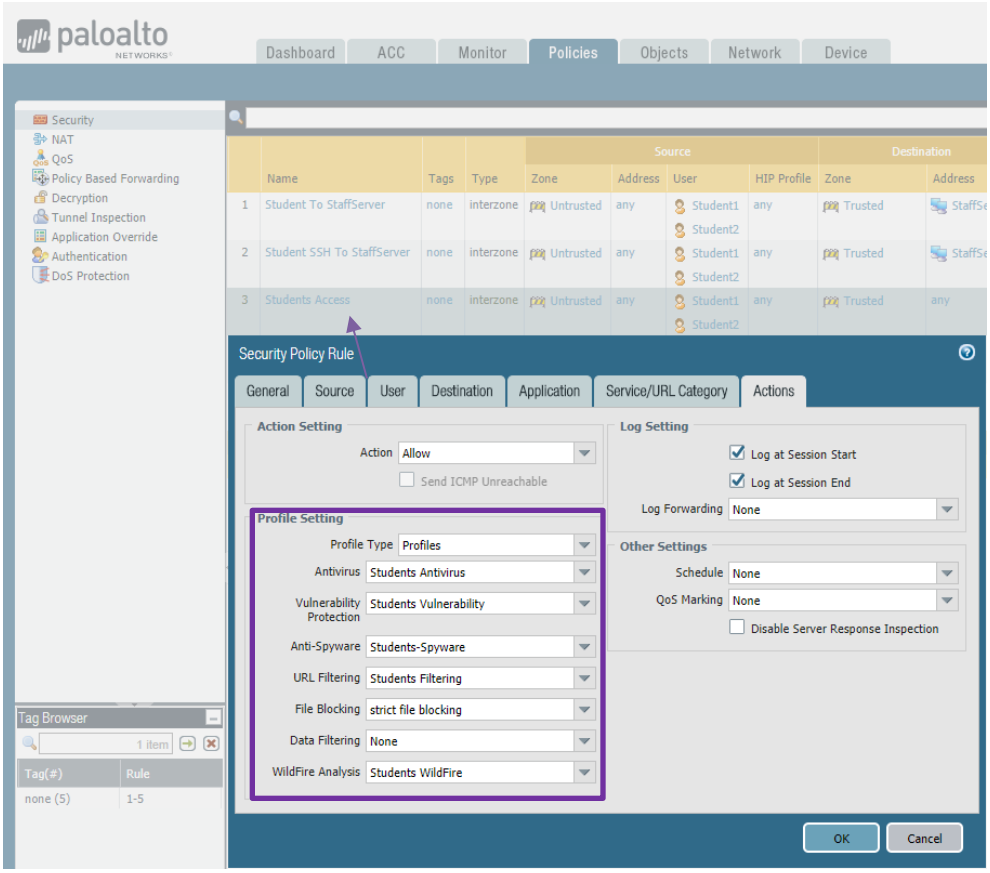


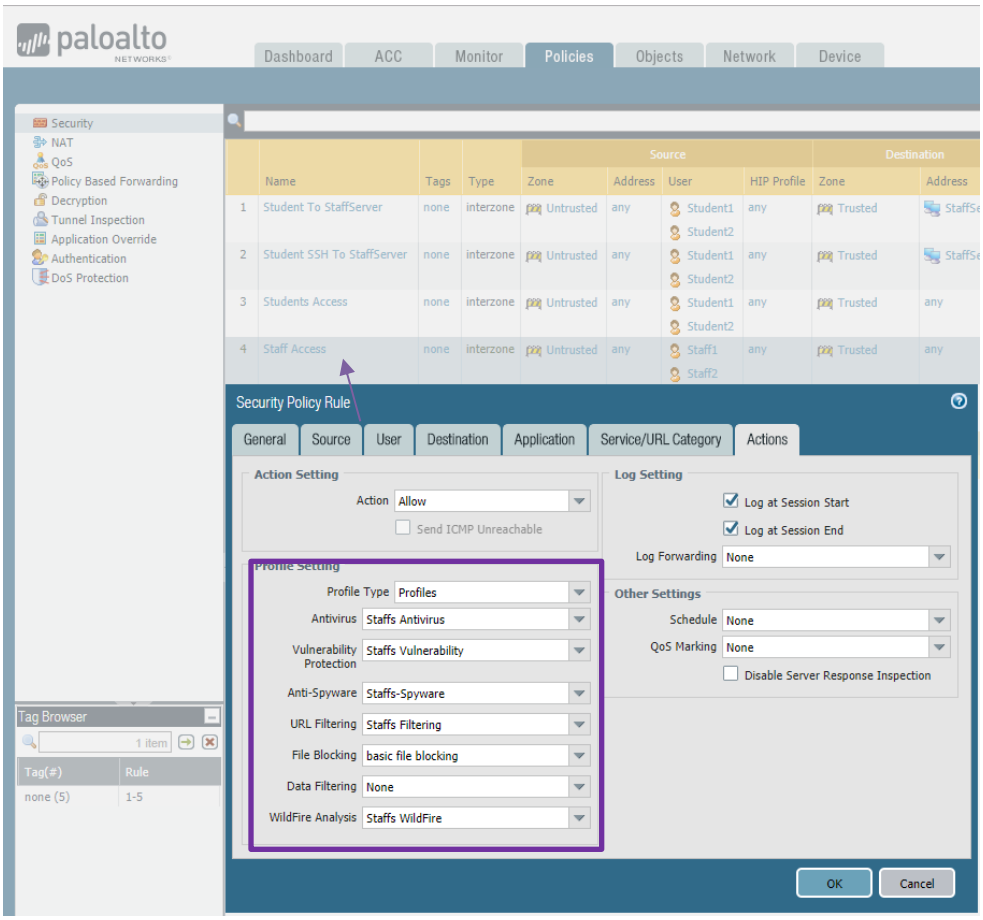


Rules are using usernames in condition and rules apply AntiVirus & URL filtering & Anti-Spyware & … specific for the Students, other settings are applied to Staff:

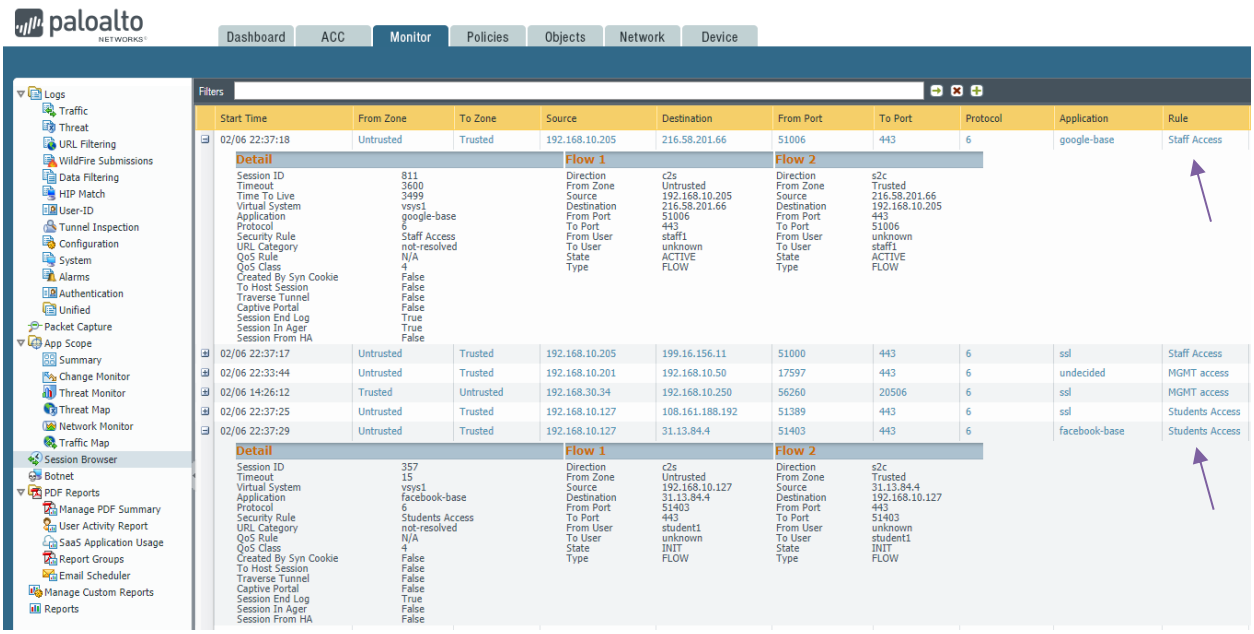


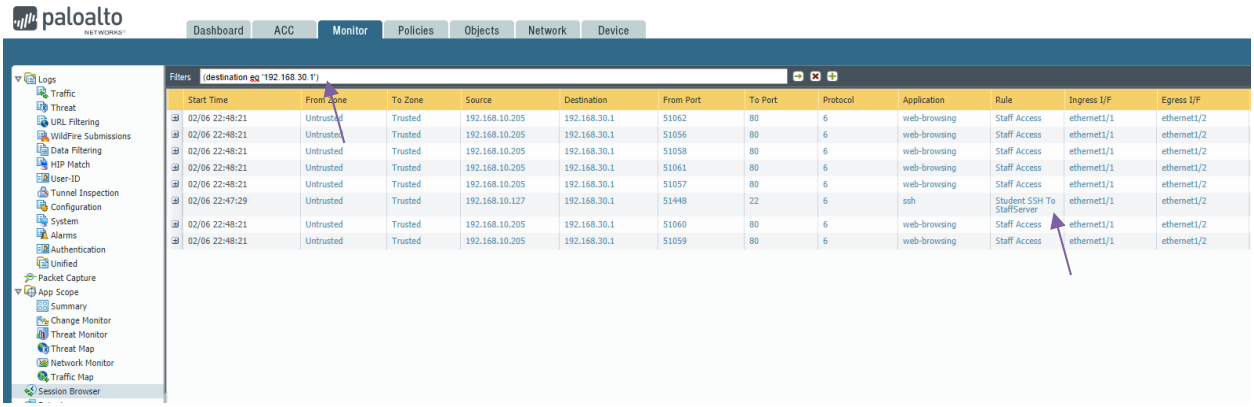
More complete picture of Firewall rules:



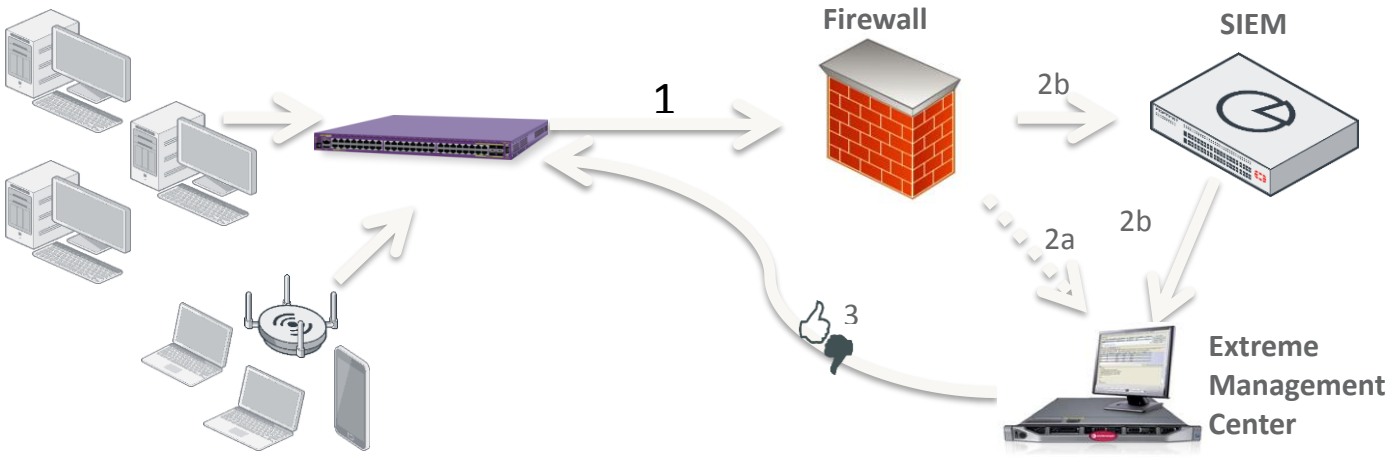


Online monitor of the rule usage:





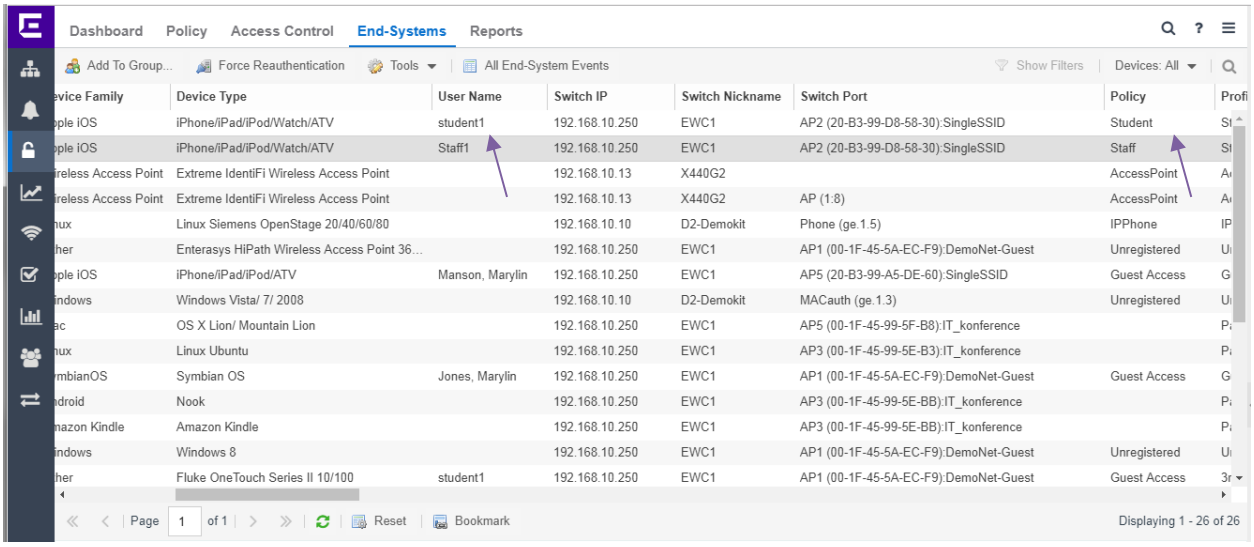
How Distributed IPS (DIPS) works – PaloAlto -> XMC



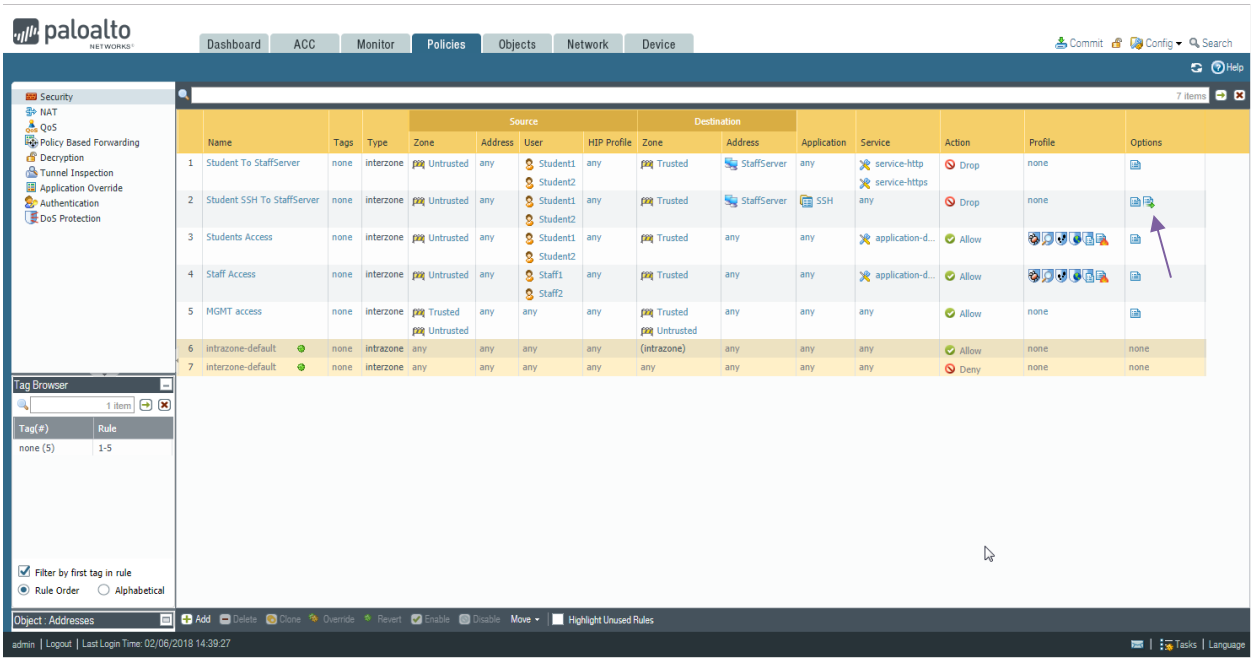
1. User traffic is analyzed by NG firewall. (Firewall, AV, AntiSpyware, URL filtering etc.)
2. Security incidents are reported to Extreme Management Center (and SIEM)
3. Extreme Management Center can apply dynamic reaction based on attributes of that security incident.
   E. g.: Quarantine the user at the network point of presence (switch, wireless AP, VPN)

DIPS: PaloAlto -> XMC

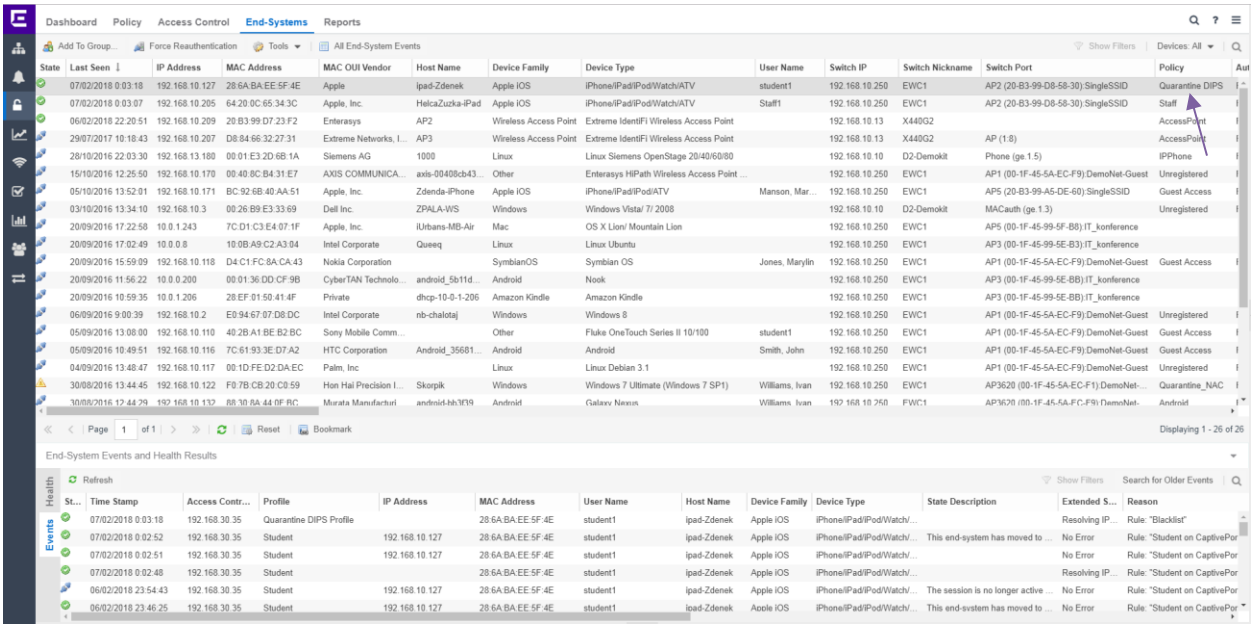
There is user “Student1” logged in to the network. The security policy profile “Student” is applied:



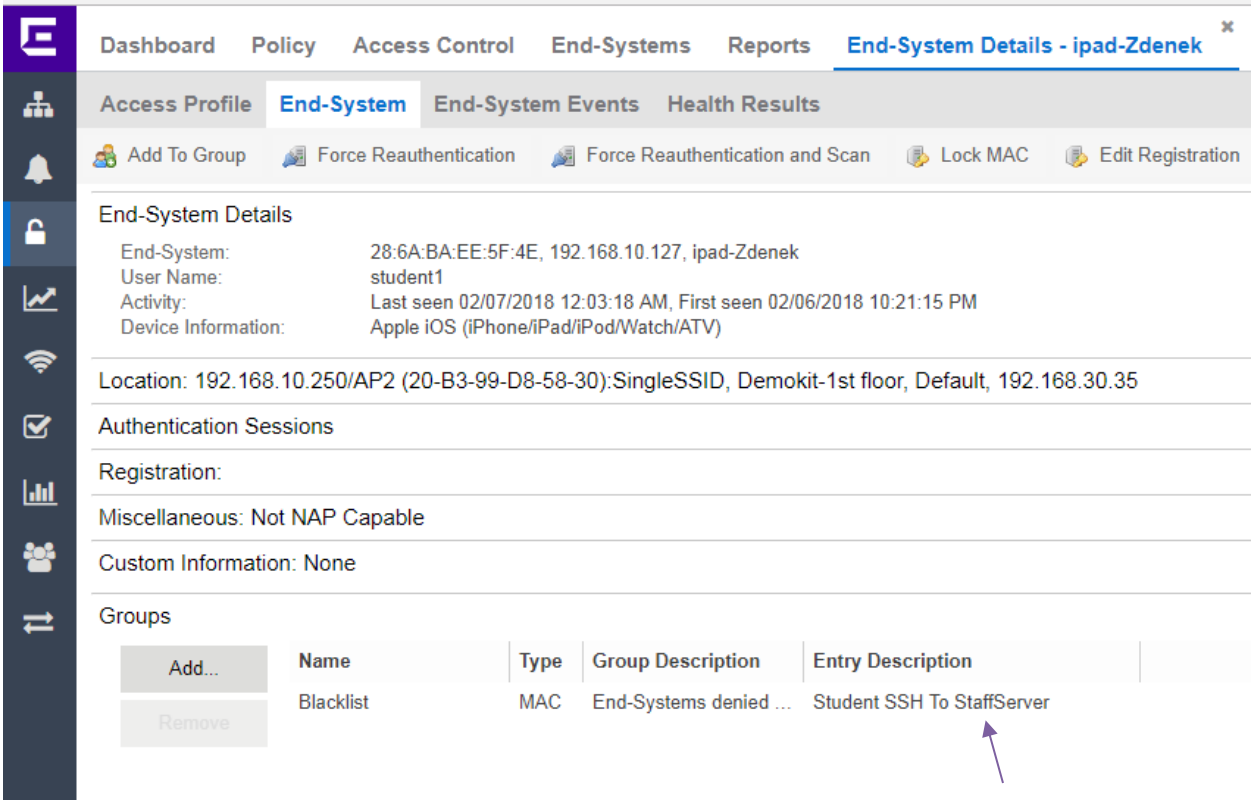
If “Student1” or “Student2” does SSH to the Staff server then the XMC is informed:



I can ping the student device. When I open SSH session from Student device to the staffserver I am quarantined:

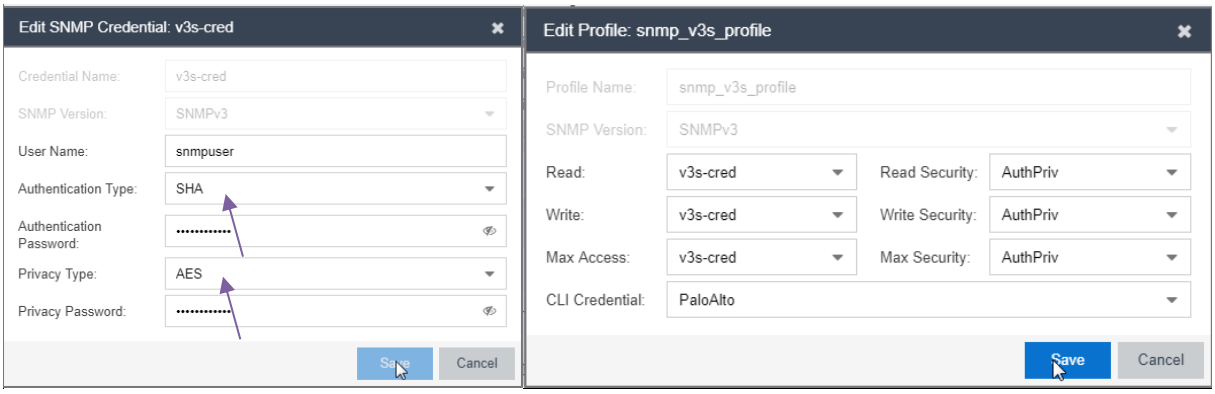


The PaloAlto rule name is part of the reason description:



Configuration options XMC

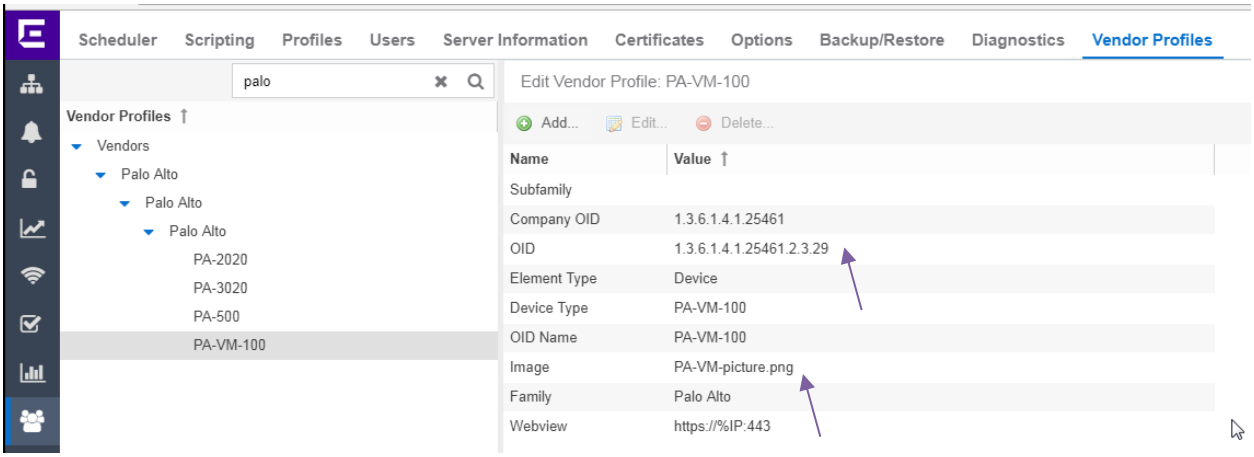
SNMP configuration (not necessary for User-ID mapping):



PaloAlto does require **Authentication Type**: SHA

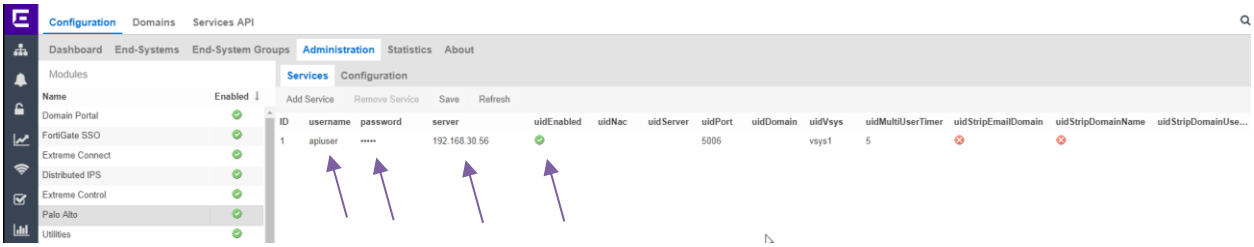
PaloAlto does require **Privacy Type**: AES

Vendor Profile configuration (beta feature in XMC version 8.0 and 8.1.1) (not necessary for User-ID mapping):



OID is SysObjectID = unique identifier for the device type. Different products does have different SysObjectID. You can determine the SysObjectID by mibtools or by XMC OneView -> Network -> right click on the device -> Device -> Configure Device -> Vendor Profile Definition

Connect configuration:



ID = you can have more PaloAlto firewalls

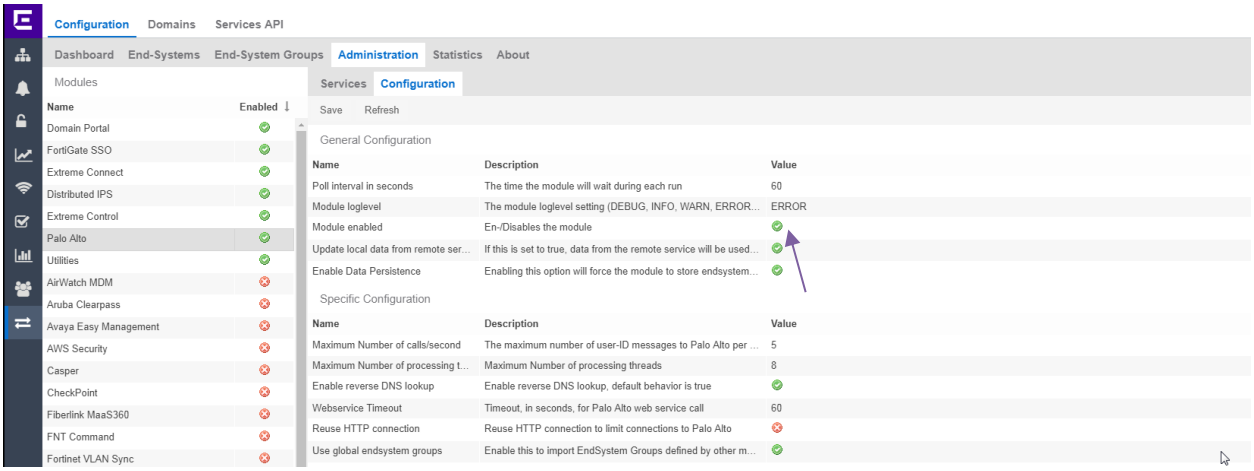
Username = username the API call will use. The username must match with the PaloAlto config.

Password = password the API call will use. The password must match with the PaloAlto config.

Server = This should be the management IP of the Palo Alto firewall.

uidEnabled = if not enabled the User-ID mapping will not work.

uidPort = default port for the agent = 5006



Poll interval in seconds = how often will PaloAlto module wait between cycles. This should stay at the default value of 60.

Module loglevel = verbosity of the PaloAlto module. Log file is standard server.log

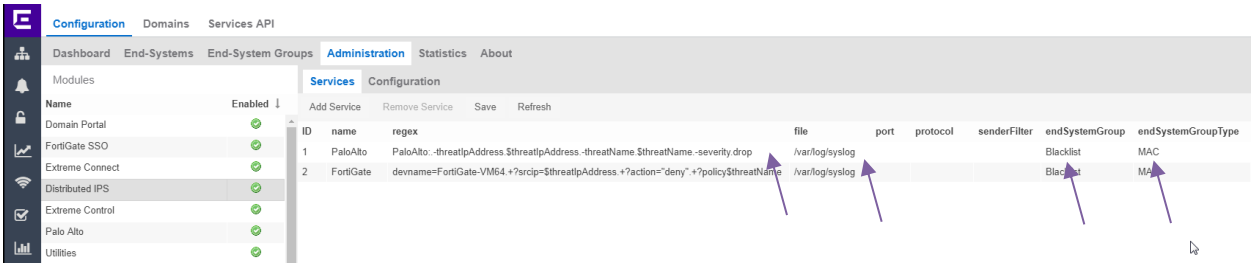
Module enabled = if you want to use this module or not.

Update local data from remote service = This should be left as true.

Enable Data Persistence = This should remain as true.

Use global endsystem groups = This should be left as true.

DIPS configuration:



ID = you can have more rules

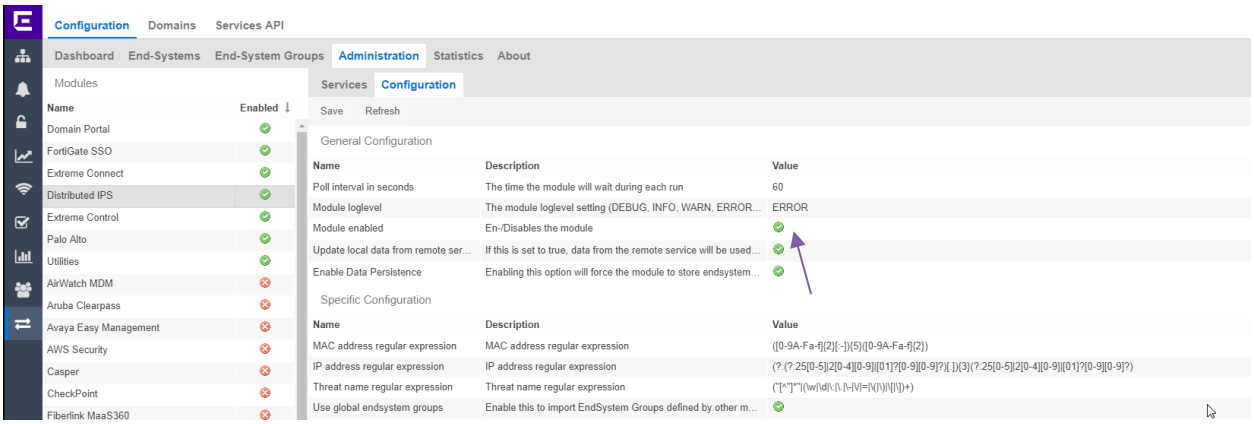
Name = name of the rule for humans

Regex = definition of what DIPS module search: PaloAlto:.-threatIpAddress.$threatIpAddress.-threatName.$threatName.-severity.drop

File = we use syslog in this case

endSystemGroup = what group will the end-system be assigned

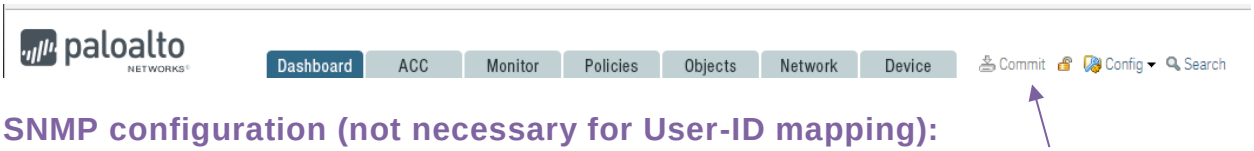
endSystemGroupType = the end-system group can be MAC or IP based…



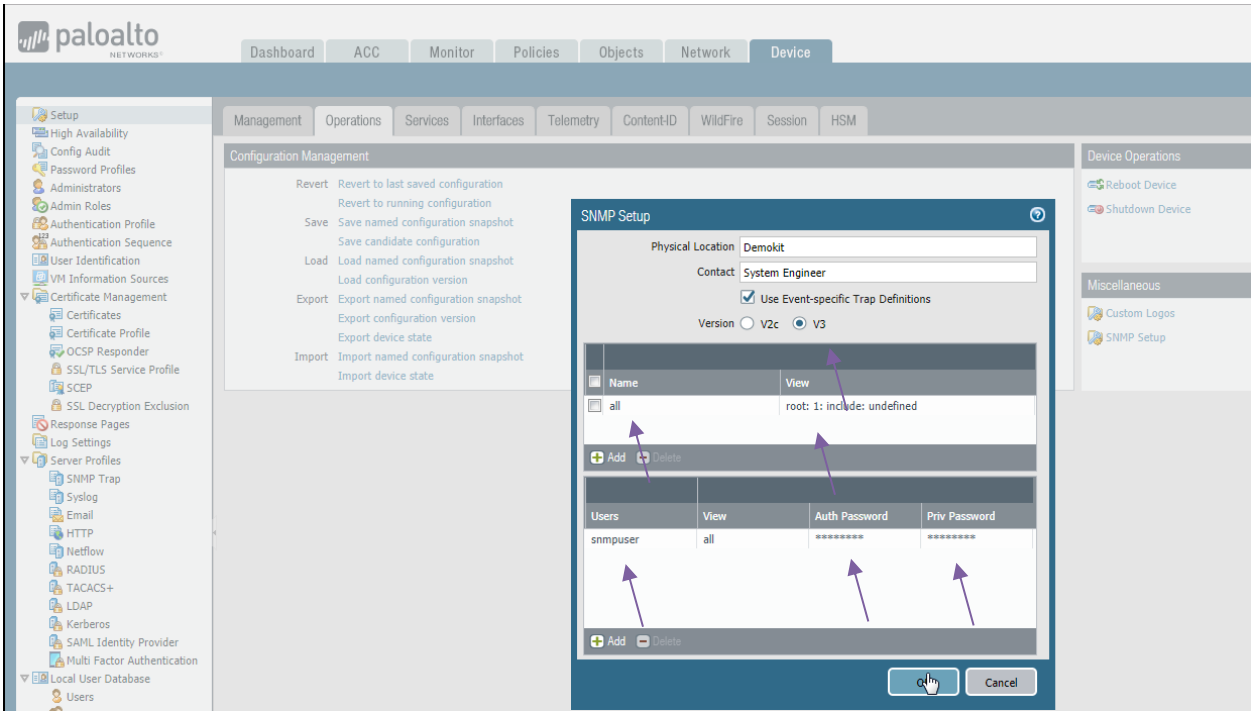
Parameters can be adjusted from the **Configuration** subtab of the Distributed IPS module. Most importantly, the **Module Enabled** value must be changed to **True**. Once the **Save** option is selected, the configuration is complete.

Configuration options PaloAlto

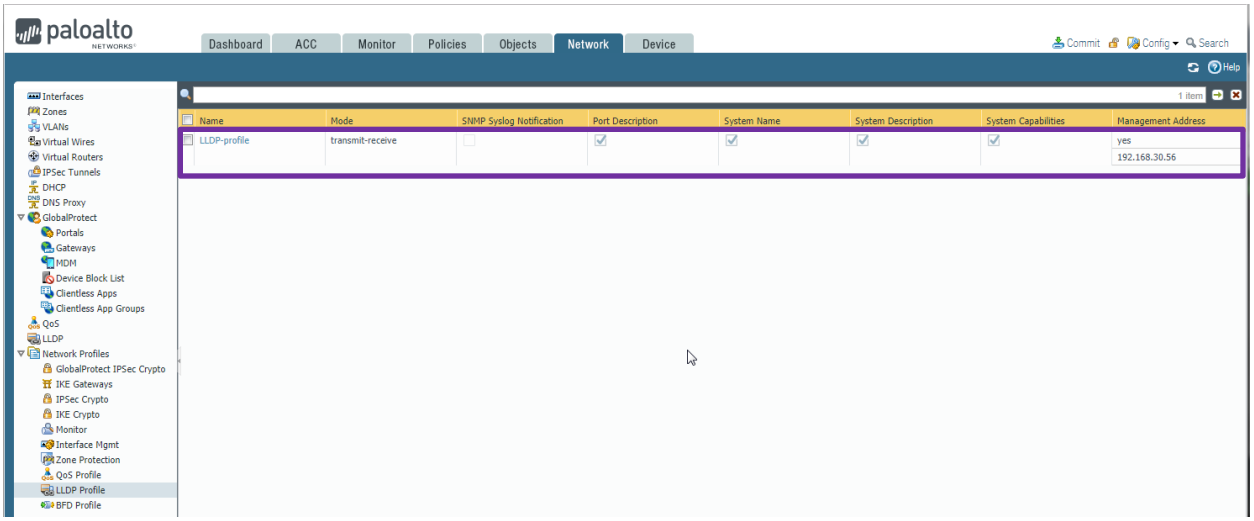
If you want changes to take effect, do not forget to commit:



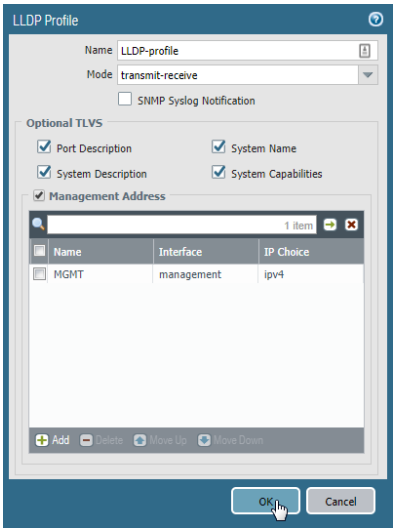
SNMP configuration (not necessary for User-ID mapping):

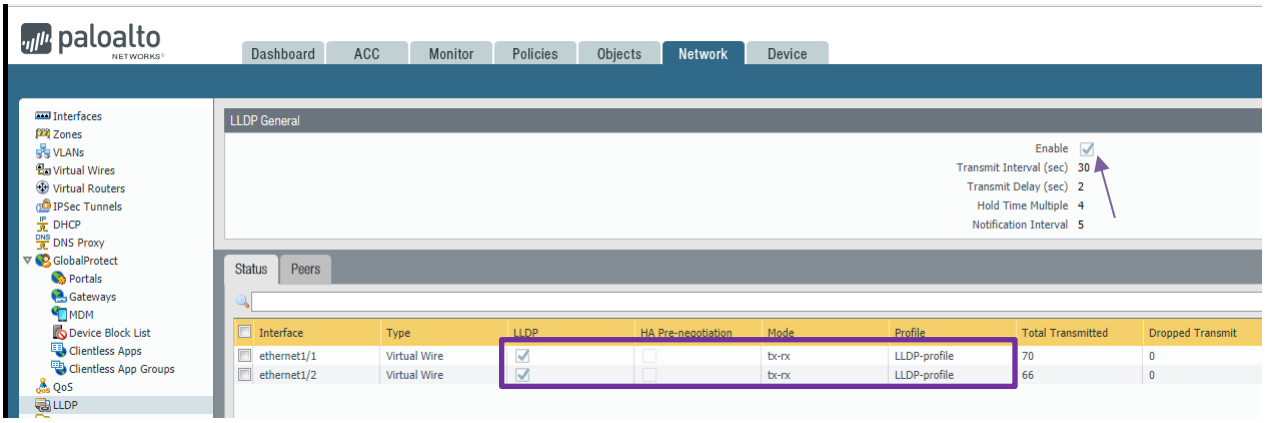


LLDP configuration (not necessary for User-ID mapping):

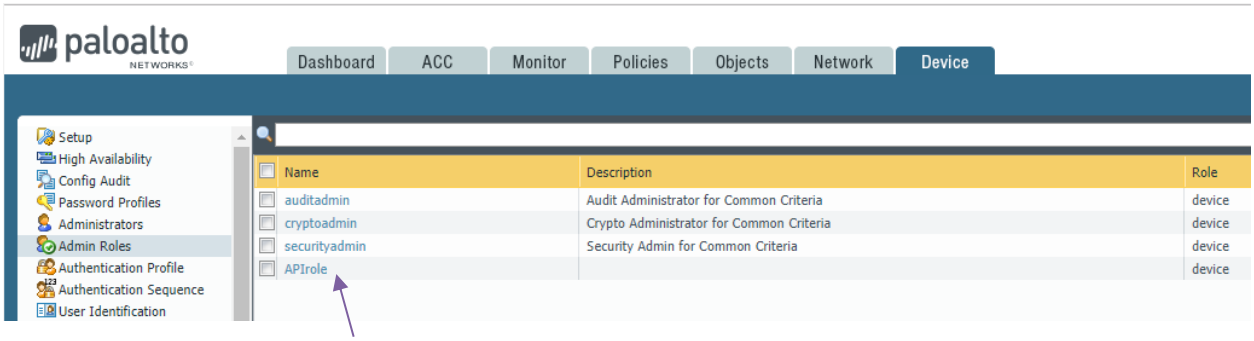


The IP in the LLDP profile should be the IP of the PaloAlto interface used for snmp.

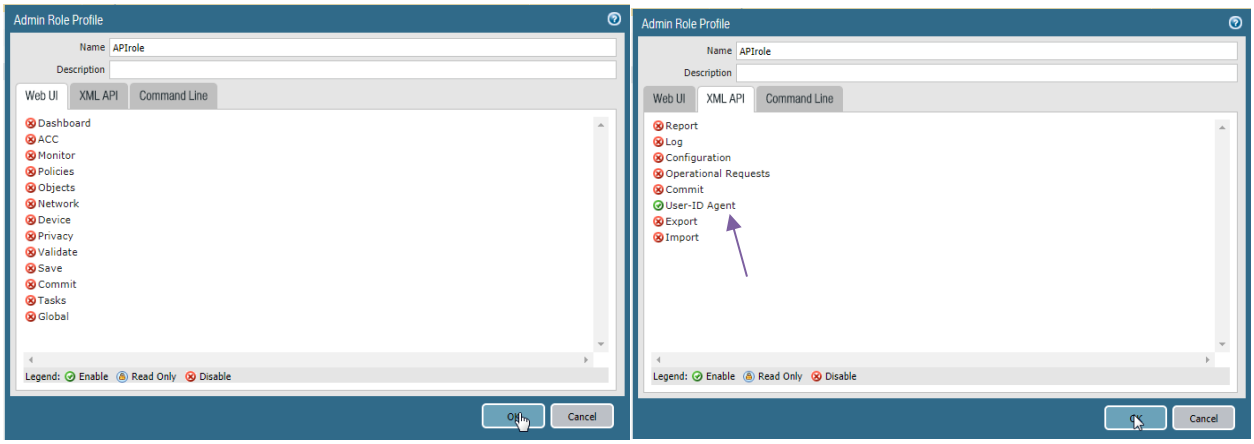




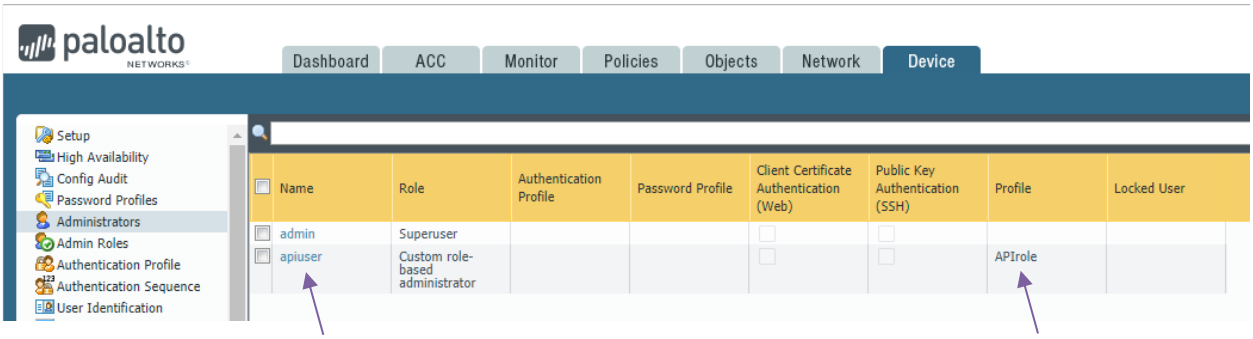
API role (for User-ID integration):



The role with authorization to call User-ID integration

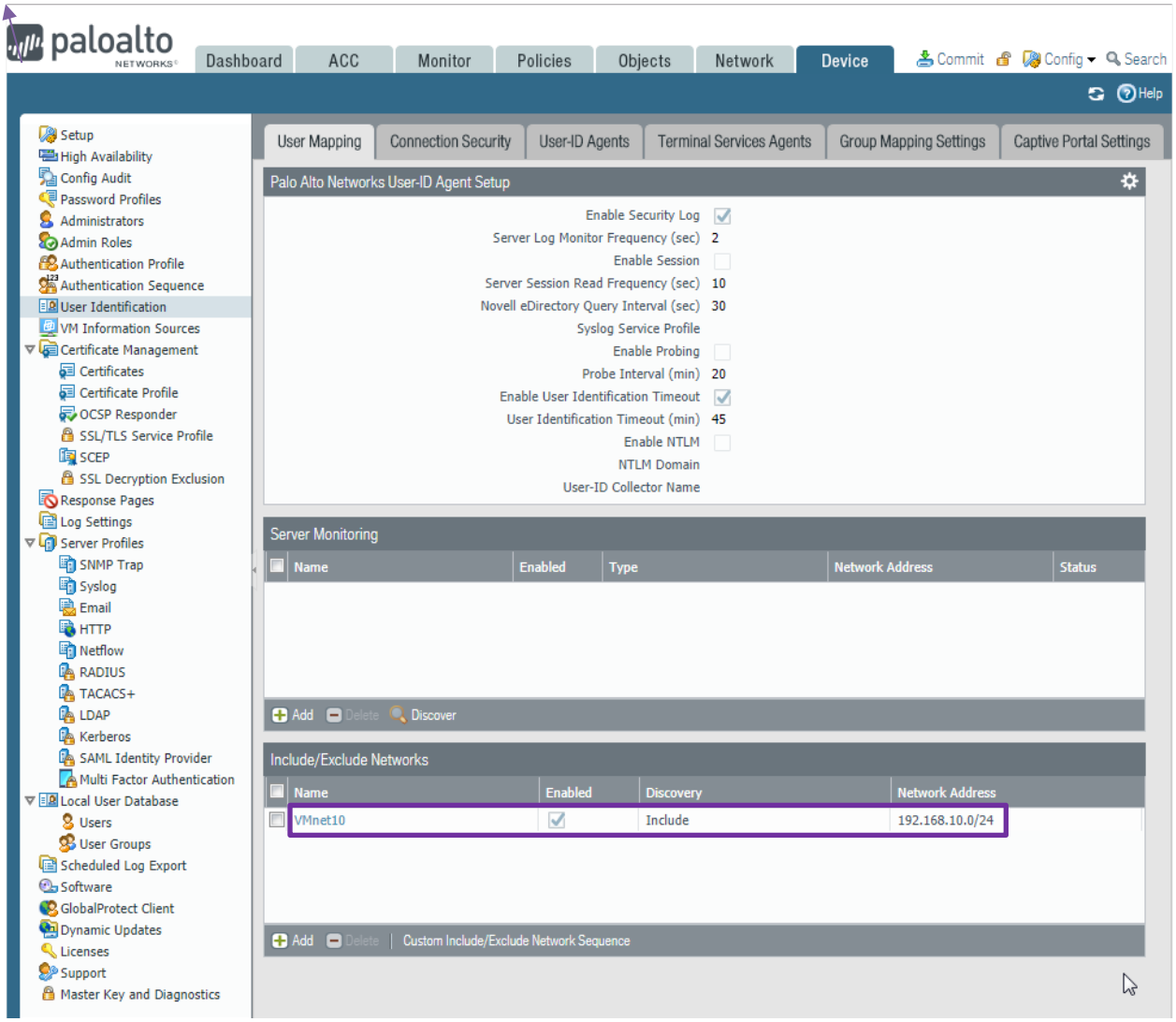


API user (for User-ID integration):



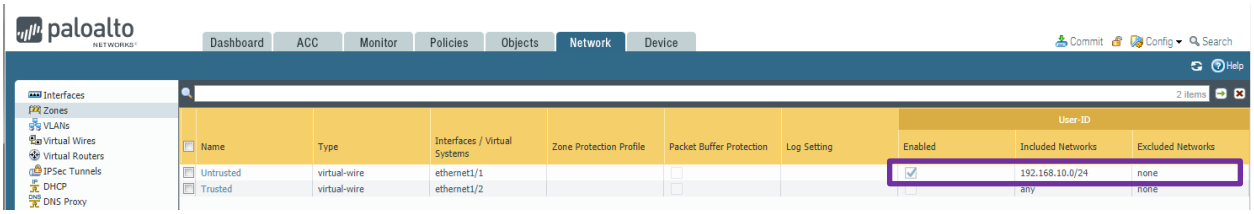
Username and password what XMC will use to update the User-ID mapping in the PaloAlto firewall.

Enable User Mapping:



Include the IP subnet to the networks where User-ID mapping will be used.

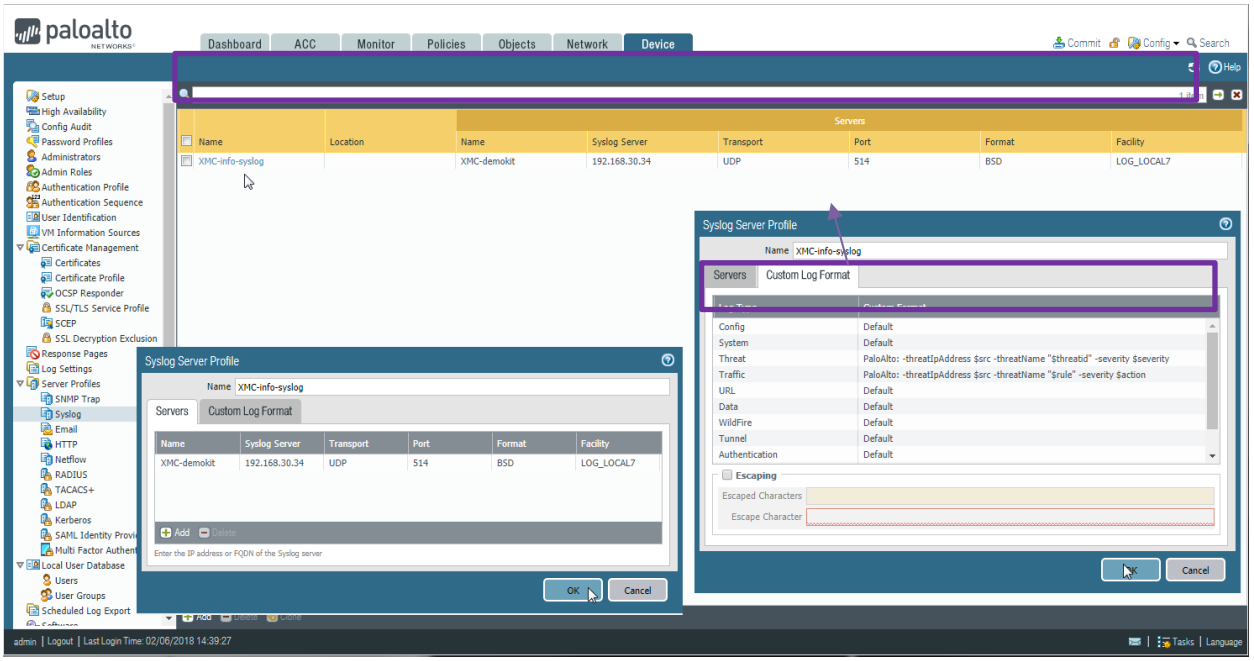
Include & enable User-ID in the Zones menu:



Zone must have User-ID enabled and assigned subnet.

DIPS configuration:

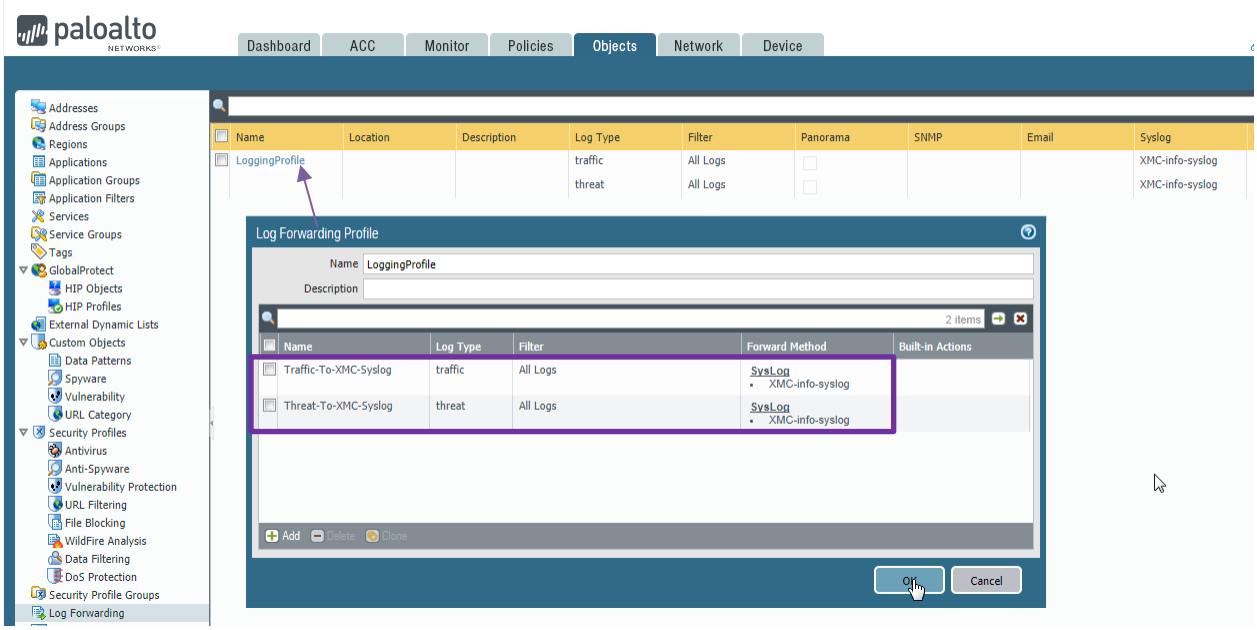
Syslog format and destination:



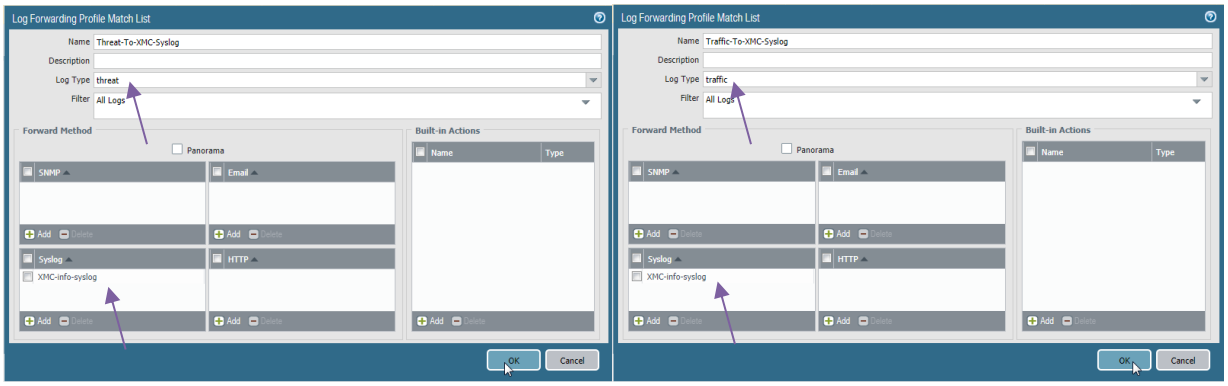
Custom format for the threat: **PaloAlto: -threatIpAddress $src -threatName "$threatid" -severity $severity**

Custom format for the traffic: **PaloAlto: -threatIpAddress $src -threatName "$rule" -severity $action**

Logging Profile definition:



Log forwarding profiles. One for traffic, one for threat. Each profile will use already defined syslog destination and format.



Terms & Condition of Use

Extreme Networks, Inc. reserves all rights to its materials and the content of the materials. No material provided by Extreme Networks, Inc. to a Partner (or Customer, etc.) may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying and recording, or by any information storage or retrieval system, or incorporated into any other published work, except for internal use by the Partner and except as may be expressly permitted in writing by Extreme Networks, Inc.

This document and the information contained herein are intended solely for informational use. Extreme Networks, Inc. makes no representations or warranties of any kind, whether expressed or implied, with respect to this information and assumes no responsibility for its accuracy or completeness. Extreme Networks, Inc. hereby disclaims all liability and warranty for any information contained herein and all the material and information herein exists to be used only on an “as is” basis. More specific information may be available on request. By your review and/or use of the information contained herein, you expressly release Extreme from any and all liability related in any way to this information. A copy of the text of this section is an uncontrolled copy, and may lack important information or contain factual errors. All information herein is Copyright ©Extreme Networks, Inc. All rights reserved. All information contain in this document is subject to change without notice.

For additional information refer to: http://www.extremenetworks.com/company/legal/terms/

Revision History

Date	Revision	Changes Made	Author
10/21/15	0.0	Initial Draft	J. Smart
02/07/18	0.9	Structure & Content based on PaloAlto version 8.0.5 and XMC version 8.1.1.41	Z. Pala
02/07/18	0.9.5	Added arrows, formatting, extended the Connect descriptions	Z. Pala